NIST National Institute of Standards and Technology • U.S. Department of Commerce
INFORMATION TECHNOLOGY LABORATORY
NO. 101 February 2008

SAFEGUARDING HEALTH CARE INFORMATION

While the electronic exchange of health care information offers major benefits to health care providers and patients alike, Americans are justifiably concerned with protecting the privacy and integrity of their electronic health information. To address these concerns, ITL's Computer Security Division and the U.S. Department of Health and Human Services (HHS), Centers for Medicare and Medicaid Services (CMS), recently cosponsored a workshop on security standards for safeguarding Electronic Protected Health Information (ePHI) as specified by the Health Insurance Portability and Accountability Act (HIPAA) of 1996. As defined by HIPAA, ePHI is any protected health information which is created, stored, transmitted, or received electronically. The conference focused on the HIPAA Security Rule, which specifies physical, technical, and administrative methods for protecting the electronic health information of individuals. Composed of health care professionals from the health care and information technology sectors, the audience discussed challenges, tips, techniques, and issues for implementing, adhering to, and auditing the requirements of the HIPAA Security Rule.

Keynote speaker Anthony Trenkle, director of CMS' Office of E-Health Standards and Services (OESS), addressed the audience on HIPAA compliance activities and CMS' plans for proactive HIPAA assessments. Representatives from NIST, the Department of Homeland Security, the HHS Office of the National Coordinator for Health IT, the Workgroup for Electronic Data Interchange, BlueShield of California, the American Medical Association, the Medical Group Management Association, and the Americas Health Insurance Plans presented on a variety of topics relevant to implementing the HIPAA Security Rule, including:

- The latest security threats to, and safeguards for, protecting electronic health information;
- The potential for automating measurement and assessment of the HIPAA Security Rule technical requirements using the Security Content Automation Protocol (SCAP);
- The Health Information Exchange (HIE) standards selection process and its impact on HIPAA;
- An industry perspective on implementing the HIPAA Security Rule; and
- The upcoming revision of NIST Special Publication 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule* (see *http://csrc.nist.gov/publications/nistpubs/800-66/SP800-66.pdf*).

Workshop presentations are at http://csrc.nist.gov/news_events/HIPAA-Jan2008_workshop/presentations.html.

Text and Video Retrieval Research Advances

ITL's Information Access Division recently hosted NIST's annual Text REtrieval Conference (TREC) and the TREC Video Retrieval Evaluation (TRECVid) Workshop. TREC and TRECVid serve the information retrieval research community and advance the state of the art in language and multimedia technologies by providing the infrastructure for large-scale evaluation of those technologies and an open forum for their discussion. TREC 2007 tracks included tasks in question answering, blog search, detecting spam in an e-mail stream, enterprise search, search in legal discovery, information access within the genomics domain, and new techniques for constructing fair test collections for very large corpora. Approximately 100 groups from 18 countries participated in the evaluation, representing organizations in academia, industry, and government. In TRECVid, 54 research teams from the Americas, Asia, Australia, and Europe completed at least one of the tasks: shot boundary detection, high-level feature extraction, search (automatic and interactive), or rushes video summarization.

TREC 2007 focused on exploring broader information contexts than previous TRECs. This was accomplished by exploring both different document genres and different retrieval tasks. Traditional TREC document genres of newswire and Web pages were still used, but these were joined by blogs, e-mail, corporate repositories, and scientific documents. Retrieval tasks included traditional ranked retrieval search as well as text categorization, focused responses, and opinion finding.

After working with broadcast news video in English, Arabic, and Chinese for four years, TRECVid confronted systems in 2007 with a new sort of data for the shot boundary, feature, and search tasks – educational, cultural, news magazine, and historical footage in Dutch from the Netherlands Archive for Sound and Vision. Much more varied in topic and less repetitive in structure, such data helped researchers gauge the significant need for adaptation of fully automatic feature extraction and search systems to the new data. Shot boundary detection approaches performed well without retraining, and interactive search systems achieved useful results

INFORMATION TECHNOLOGY LABORATORY

If you are interested in receiving our newsletter, send your name, organization, and business mailing address to:

ITL Newsletter
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900

You will be placed on this mailing list only.

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of new information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov.

ITL Editor: Elizabeth B. Lennon
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900
Phone: (301) 975-2832
Fax: (301) 975-2378
E-mail: elizabeth.lennon@nist.gov

despite the change in test data. The video summarization task used unedited video from several BBC dramatic series and asked systems to eliminate redundancy due to retakes and present the summary so that identifying significant objects, people, and events was as easy as possible. The Web site is http://trec.nist.gov.

Research on Suspensions Featured at Supercomputing Conference

Results of a NIST team's research on the flow of suspensions (mainly concrete), carried out with a 2006 NASA award of 1,000,000 CPU hours on the Columbia supercomputer at the NASA Ames Research Center, were demonstrated at the NASA and NIST booths at the Supercomputing 2007 conference held in Reno, Nevada. This is the main conference in the United States showcasing research enabled by massively parallel computing. The simulations use dissipative particle dynamics (DPD) to simulate the actual flow and interaction of solid particles in a fluid matrix. State-of-the-art real-time visualization based on non-photorealistic rendering and graphical processing unit (GPU) programming facilitated exploration of the rheology simulation output. At the NASA booth, these visualizations were shown on a large 3x3 array of monitors. The results demonstrated advances in understanding the influence of finite size effects, stress transmission, time scales, and system equilibration for both spherical particles and real-shape particles of gravel and sand. This work was carried out by a team of researchers in ITL's Mathematical and Computational Sciences Division and the Materials and Construction Research Division of NIST's Building and Fire Research Laboratory.

Following this very successful research, the NIST team has been granted an additional 400,000 hours by NASA. This new time will be used for two projects. First, the team will extend the previous rheology study to include a broader shape and size distribution of aggregates. Second, they will start the study of the scalability of their parallel code (called HydratiCA), which simulates the three-dimensional changes in the structure and chemical composition of aqueous mineral systems, such as those encountered in environmental geochemistry, ceramic processing, and cement-based materials. The ultimate goal is to combine both the DPD and HydratiCA codes into a single program that models the flow, chemistry, and microstructure of concrete and other complex materials.

Call for Participation in Usability Benchmark Testing of Voting Equipment

A recent *Federal Register* notice invited voting equipment manufacturers to participate in Phase II of ITL's usability benchmark testing. The four primary manufacturers of voting equipment, Diebold, ES&S, Hart Intercivic, and Sequoia, provided voting equipment for ITL's Phase I research. The research is designed to (1) determine the realistic usability benchmarks for current and future voting system technology to support usability performance standards in next-generation voluntary voting systems standards; and (2) develop usability test protocols for conformance testing of such standards. ITL may also examine relevant instructions, documentation, and error messages, without doing any direct usability studies thereon. The *Federal Register* notice has been posted on NIST's voting Web site at http://vote.nist.gov/FRNVotingPhaseII.pdf.

SELECTED NEW PUBLICATIONS

User's Guide to Securing External Devices for Telework and Remote Access
By Karen Scarfone and Murugiah Souppaya
NIST Special Publication 800-114
November 2007
http://csrc.nist.gov/publications/nistpubs/800-114/SP800-114.pdf

This publication helps teleworkers secure the external devices they use for telework, such as personally owned and privately owned desktop and laptop computers and consumer devices (e.g., cell phones, personal digital assistants [PDAs]). The document focuses specifically on security for telework involving remote access to their organizations' nonpublic computing resources. It provides practical, real-world recommendations for securing telework computers' operating systems and applications, as well as home networks that the computers use.

Guide to Storage Encryption Technologies for End User Devices
By Karen Scarfone, Murugiah Souppaya, and Matt Sexton

NIST Special Publication 800-111
November 2007
http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

This publication explains the basics of storage encryption, which is the process of using encryption and authentication to restrict access to and use of stored information. The appropriate storage encryption solution for a particular situation depends primarily upon the type of storage, the amount of information that needs to be protected, the environments where the storage will be located, and the threats that need to be mitigated. The publication describes three types of solutions and makes recommendations for implementing and using each type.

Guidelines on Securing Public Web Servers
By Miles Tracy, Wayne Jansen, Karen Scarfone, and Theodore Winograd
NIST Special Publication 800-44 Version 2
September 2007
http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf

This document assists organizations in installing, configuring, and maintaining secure public Web servers. Topics include choosing Web server software and platforms, securing the underlying operating system and Web server software, deploying appropriate network protection mechanisms, and using, publicizing, and protecting information in a careful and systematic manner. The publication also provides recommendations for maintaining secure configurations through patching and upgrades, security testing, log monitoring, and backups of data and operating system files.

Investigating Resource Allocation in a Standards-Based Grid Compute Economy
By Christopher Dabrowski
NISTIR 7463
November 2007
http://www.itl.nist.gov/div897/publications/NISTIR7463.pdf

This paper reports work investigating resource allocation in a simulated grid compute economy where consumers and providers employ software components implemented with emerging Web Services and grid standards. The investigation employs a model to simulate interactions between large numbers of consumers and providers where both parties dynamically enter into contracts to allocate resources. A series of trials is conducted to vary provider criteria for accepting contracts to compare performance using profit-based criteria to performance using more traditional criteria guided by system utilization under conditions of moderate load and overload. The results show that a grid computing economy, in which consumers and providers attempt to maximize individual monetary profit, can produce resource allocations using standards-based components that are not only efficient and benefit direct participants economically, but are also beneficial to the larger community that depends upon the computing grid.

Security Biometric Match-on-Card Feasibility Report
By David Cooper, Trung-Hung Dang, Philip Lee, William MacGregor, and Ketan Mehta
NISTIR 7452
November 2007
http://csrc.nist.gov/publications/nistir/ir7452/NISTIR-7452.pdf

This document publishes the results of the secure Biometric Match-on-Card feasibility study. Researchers conducted the study to understand the effects of security on performance of Personal Identity Verification (PIV) authentication transaction. The report describes the tests that were conducted to obtain timing metrics for the feasibility study and provides a summary of test results.

MARK YOUR CALENDAR

7th Symposium on Identity and Trust on the Internet (IDtrust 2008)
Dates: March 4-6, 2008
Place: NIST, Gaithersburg, Maryland
Sponsors: NIST, Internet 2, Organization for the Advancement of Structured Information Standards (OASIS) and Federal Public Key Infrastructure Policy Authority (FPKIPA)

Theme: Identity and Trust Infrastructures: This symposium will bring together academia, government, and industry to explore all aspects of identity and trust. Previously known as the PKI R&D Workshop (2002-2007), the new name reflects interest in a broader set of tools and the goal of an identity layer for the Internet. The goal is to get practitioners in different sectors together to apply the lessons of real-world deployments to the latest research and ideas on the horizon.

NIST contact: Tim Polk, 301/975-3348, william.polk@nist.gov
Conference Web site:
http://middleware.internet2.edu/idtrust

21st Annual Federal Information Systems Security Educators' Association (FISSEA) Conference
Dates: March 11-13, 2008
Place: NIST, Gaithersburg, Maryland
Sponsors: NIST and FISSEA

With a theme of *Security Through Innovation and Collaboration*, this year's FISSEA conference will provide dual tracks of high-quality presentations, great networking opportunities, and vendors providing service information. Security awareness, training, and education practitioners can discover new ways to improve their IT security programs. Attendees can gain awareness and training ideas and resources, obtain practical solutions to training problems, and earn Continuing Professional Education (CPE) credits.

NIST contact: Mark Wilson, 301/975-3870, mark.wilson@nist.gov
Conference Web site: http://csrc.nist.gov/organizations/fissea/2008-conference/

Applications of Pairing-Based Cryptography: Identity-Based Encryption and Beyond
Dates: June 3-4, 2008
Place: NIST, Gaithersburg, Maryland
Sponsor: NIST

This workshop will bring together academia, government, and industry to explore innovative and practical applications of pairing-based cryptography. Pairings have been used to create identity-based encryption schemes, but are also a useful tool for solving other cryptographic problems. We hope to encourage the development of new security applications and communication among researchers, developers, and users. In addition to presentations, the workshop will facilitate panel discussions among invited experts and workshop participants.

NIST contact: Andrew Regenscheid, 301/975-5155, andrew.regenscheid@nist.gov
Conference Web site: http://www.nist.gov/ibe/

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

"ITL" Available Via E-Mail
We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send and e-mail message from your business e-mail account to listproc@nist.gov with the message subscribe itl-newsletter, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message HELP. To have the newsletter sent to an e-mail address other than the FROM address, contact the ITL editor.